RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: PART4-W01

Bridging Data and Identity: The Key to Cyber Resilience

Hema Mohan
Senior Director, Product Management, Rubrik

Joe Hladik
Head of Rubrik Zero Labs, Rubrik

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Identity is the threat vector
01
02
Data is the prize

23andMe 2022 Breach

ENTRY POINT

Credential stuffing → password reset on a real user's Okta account.

ESCALATION

Attackers escalated access using Okta integration to enroll devices, gain admin rights.

BREACH

No advanced exploit needed — **one phone call and an identity gap** enabled the breach.

DAMAGE

Ransomware followed, **multi-day outage**, stolen customer data, **$100M+ business impact**.

Agenda

01

Why identity and data are so vulnerable

02

Blind spots with existing tools

03

The advantage of unifying identity and data

04

What you can do to close the gap

Identity & Data: Twin Challenges

Identity

Massive growth in **identities**

Increasingly complex hybrid and multi-cloud **identity** environment

Rapidly increasing attacks on **identity**

Data

Massive growth in **data**

Increasingly complex hybrid and multi-cloud **data** environment

Rapidly increasing attacks on **data**

NHIs - Expanding Attack Surface

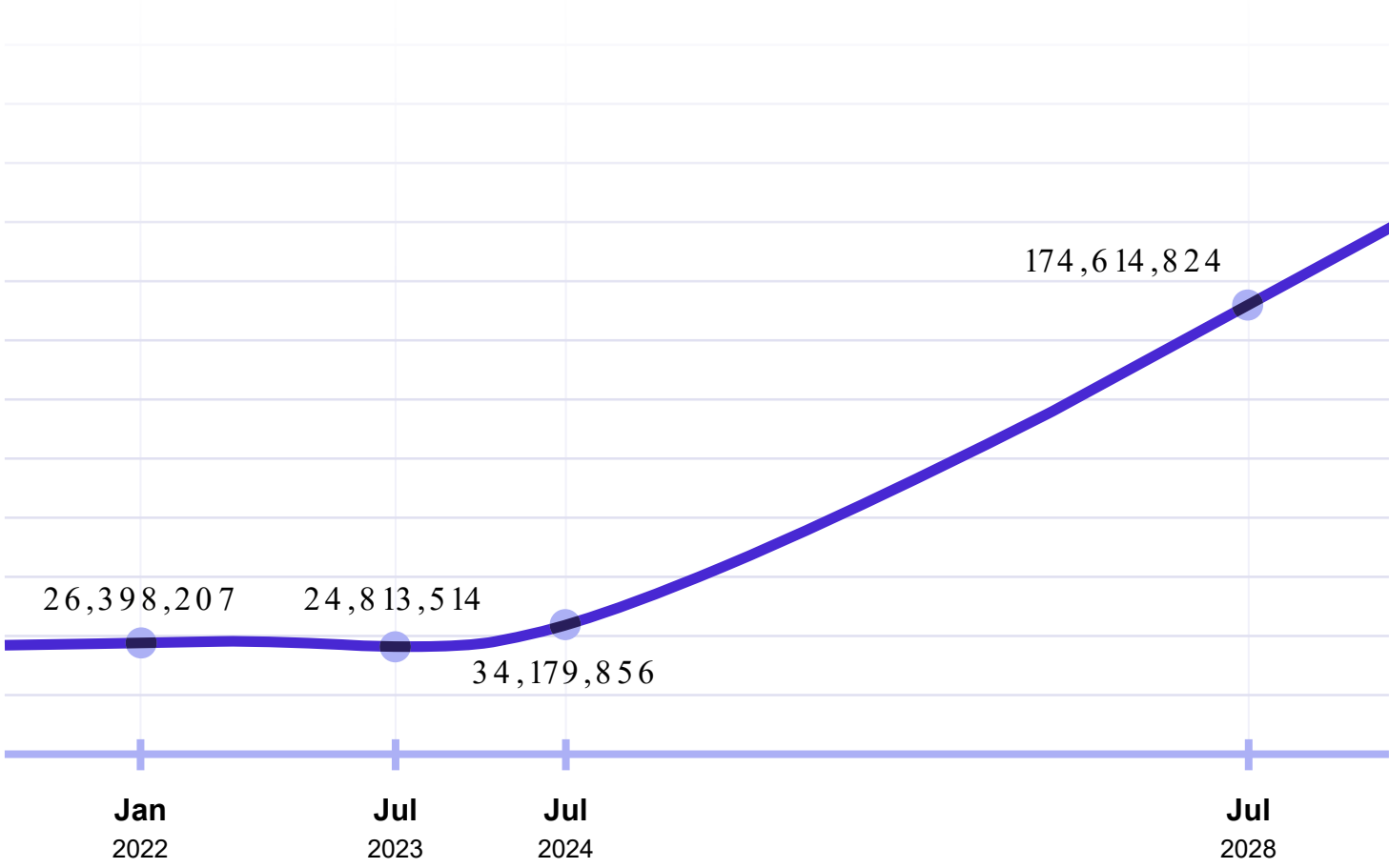
50:1 → 200:1

The ratio of NHIs to human identities is increasing

240% **growth in human and non-human identities over next 12 months**

Sensitive Data by the Numbers

A typical organization is projected to have **more than 10 million new** sensitive data records to secure in one year. This number grows by more than **150 million new** sensitive data records five years from today.



What Does the Data Landscape Look Like?

90% of IT and security leaders said they are managing hybrid cloud environments.

50% of all IT and security leaders reported that they're managing mostly cloud and SaaS-based workloads vs. on-premises workloads.

92% of IT and security leaders surveyed said they are using anywhere between 2 and 5 cloud and SaaS platforms for data storage, applications, and services.

66% of IT and security leaders surveyed said they are planning to shift toward using more cloud and SaaS-based services over the next year while 31% will maintain their ratio of hybrid cloud and on-premise environments.

Rising Challenges in Identity & Data Security

50%

experienced an AD attack in the last two years[3]

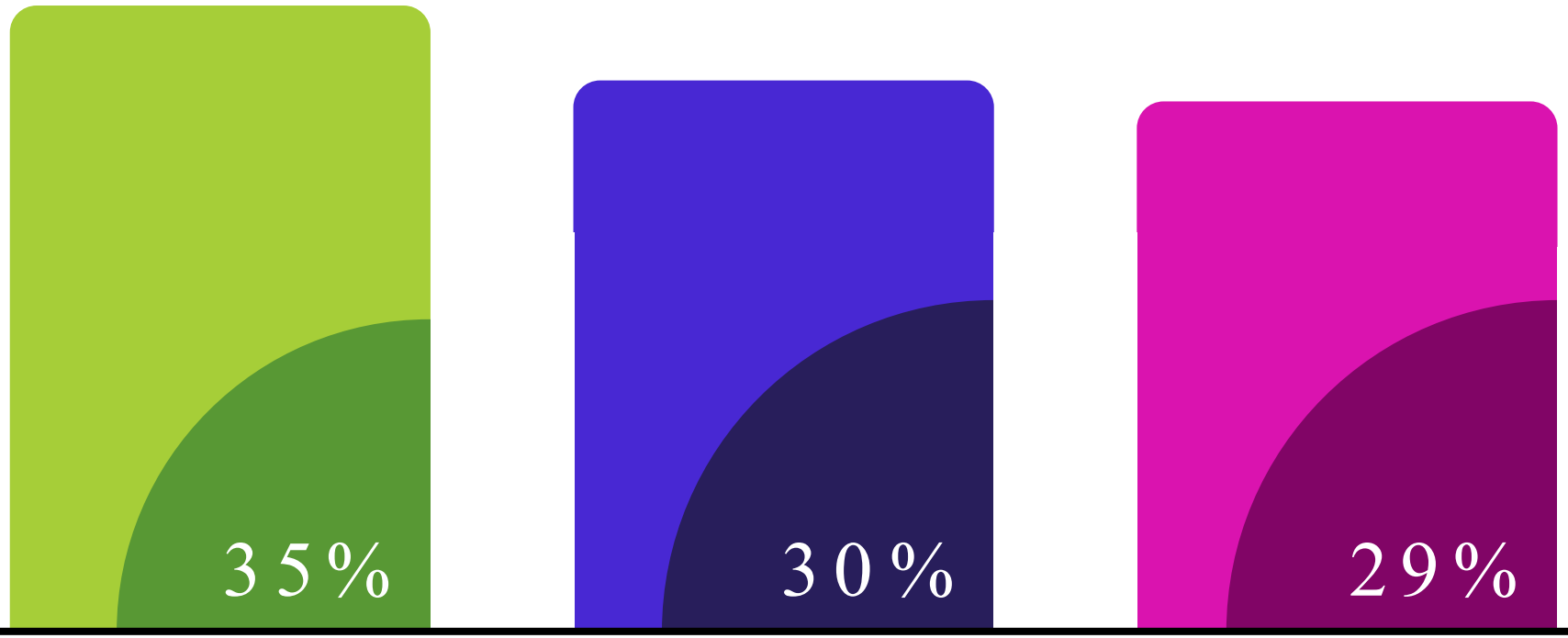
600 million

identity-based attacks are blocked by Microsoft alone on a daily basis

98%

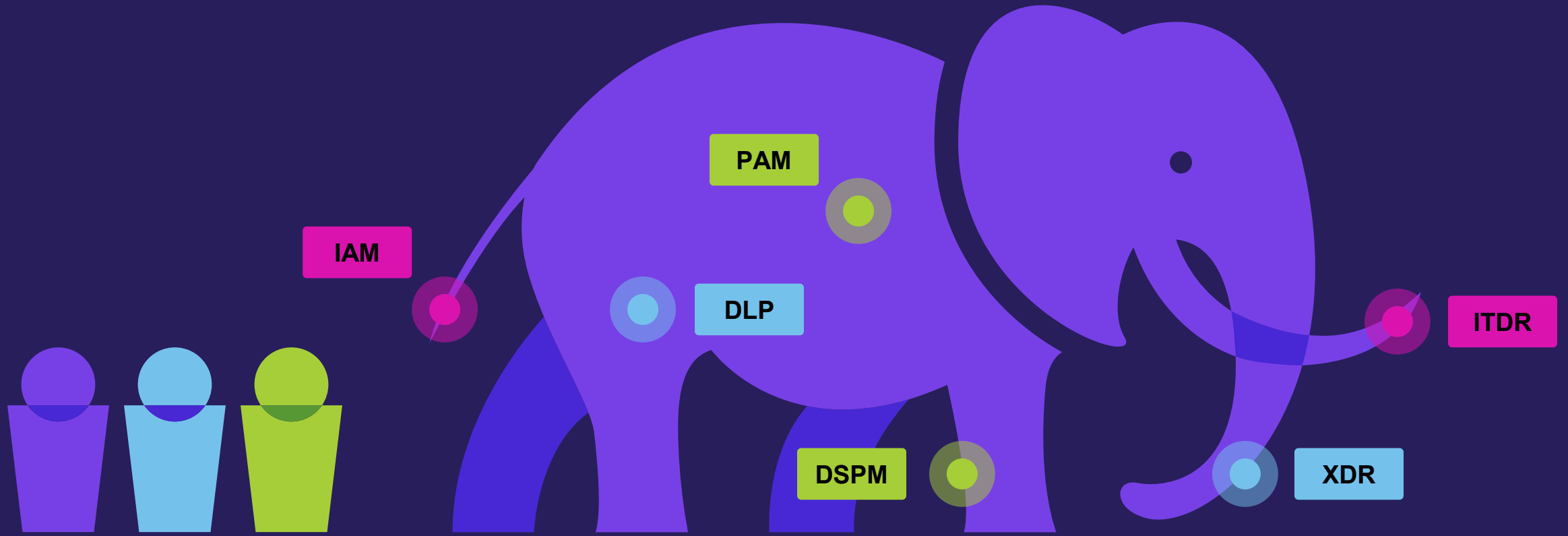
of organizations report significant data visibility challenges[1]

IT Leaders Face Challenges in Three Categories

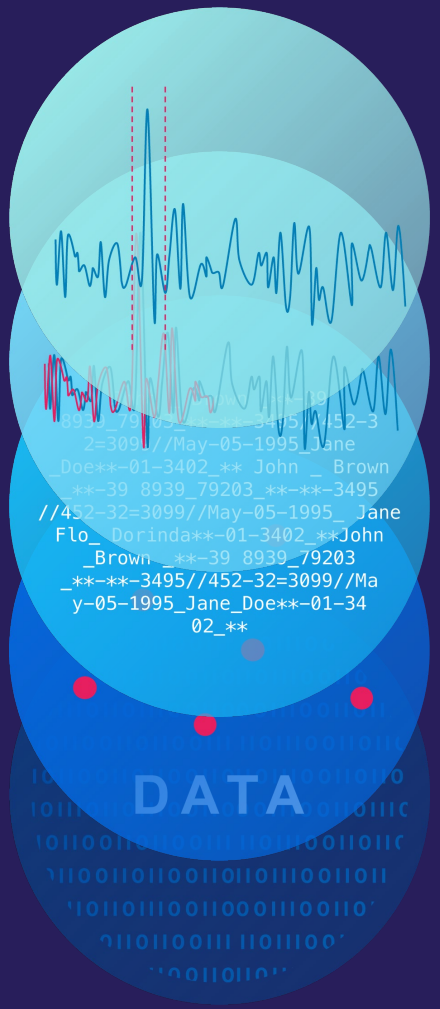


We're not missing tools

We're missing context



Secrets Your Data and Identity Share



- Where your data is stored?
- Where your data is located?
- What type of data you have?
- What is in your data?
- Who has access to your data?
- How your data is changing?
- Who is changing your data?
- Who is accessing your data?

Security Needs to Operate Before, During & After an Attack

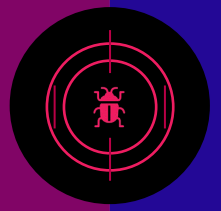
BEFORE

01

Monitor at-risk resources and users

02

Identify and reduce risk



DURING

03

Limit spread of cyber attacks

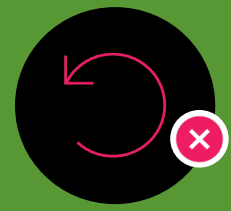
AFTER

04

Find malware and quarantine

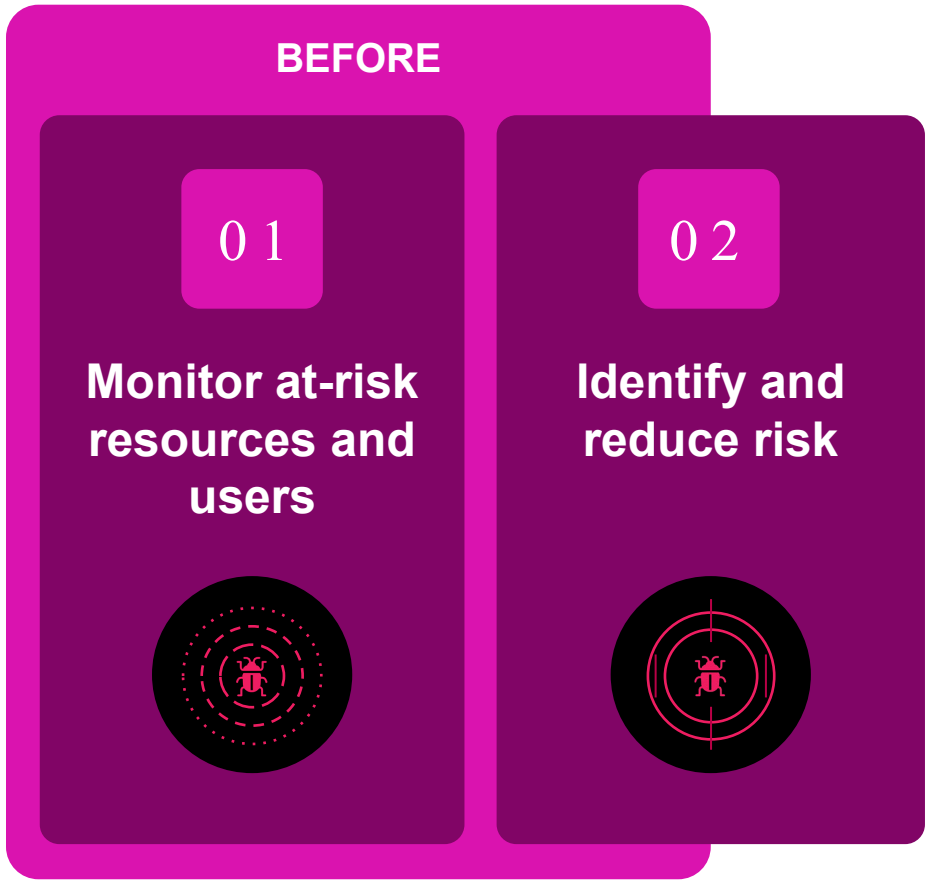
05

Restore from backup



Before an Attack

Reduce Exposure & Strengthen Security Posture



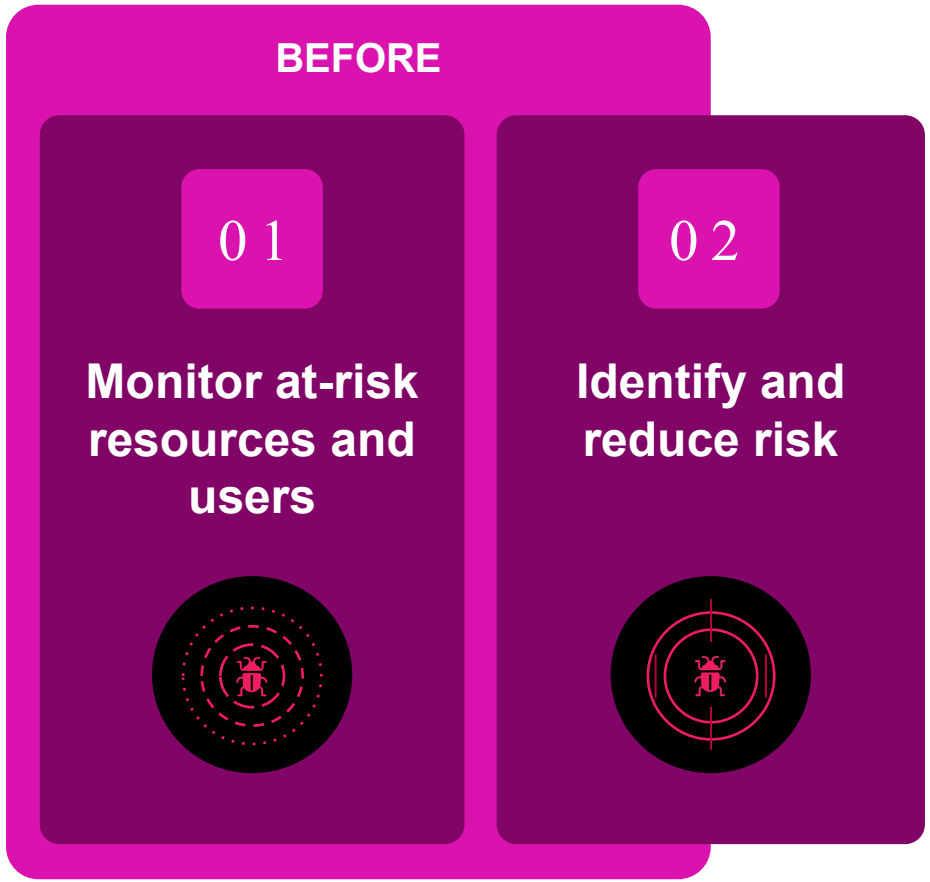
01 **Visibility**

02 **Hygiene**

03 **Posture**

Before an Attack

Reduce Exposure & Strengthen Security Posture



01 Visibility

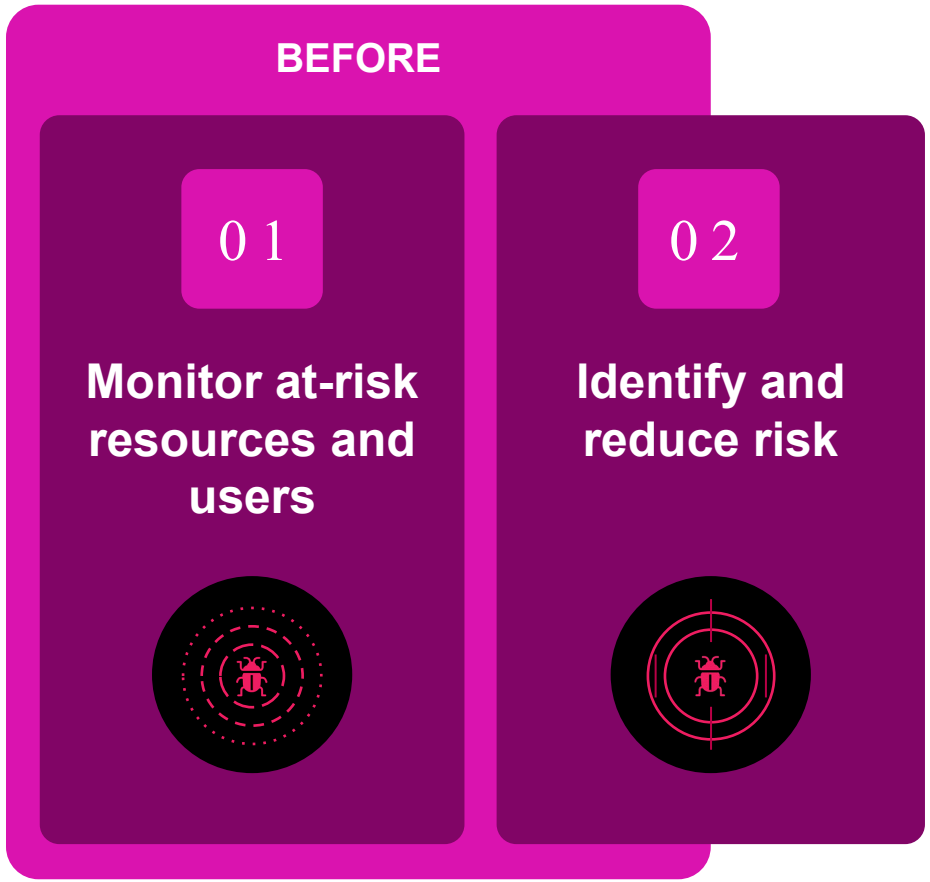
- What accounts have VPN access?
- Which service accounts exist, and what systems they can access?
- Where sensitive source code and internal IP live—and who can access it.

02 Hygiene

03 Posture

Before an Attack

Reduce Exposure & Strengthen Security Posture



01 Visibility

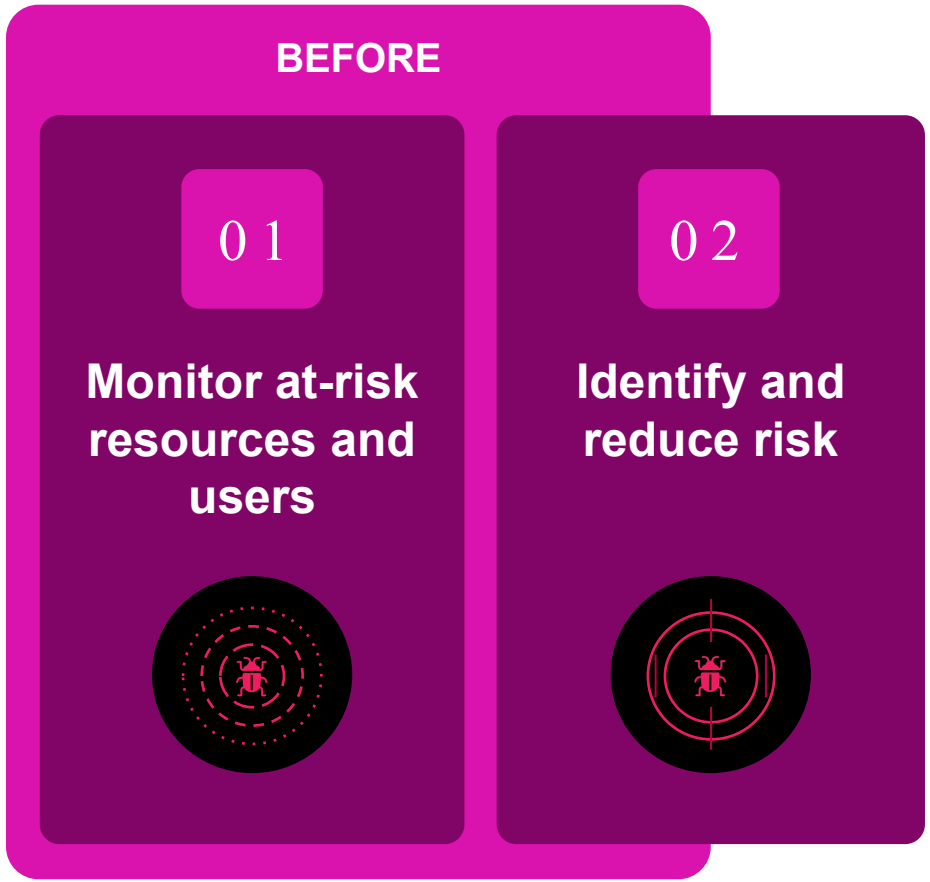
02 Hygiene

- Enforcing MFA, not optional.
- Disable or deleting stale accounts.
- Identifying and right-sizing over-permissioned service accounts.

03 Posture

Before an Attack

Reduce Exposure & Strengthen Security Posture



01 Visibility

02 Hygiene

03 Posture

- If this identity were compromised, *what could it access?*
- If this data store were exposed, *how much damage could be done?*

During the Attack

Detect, Contain, Respond Faster

01 **Stronger Signal**

02 **Prioritized Response**

03 **Containment**

During the Attack

Detect, Contain, Respond Faster

01 Stronger Signal

- A user suddenly accessing sensitive IP or they've never touched before.
- Elevated privileges granted outside normal workflows.
- Lateral movement between internal tools and AD.

02 Prioritized Response

03 Containment

During the Attack

Detect, Contain, Respond Faster

01 Stronger Signal

02 Prioritized Response

- Not just an endpoint issue.
- The identity involved now has access to high-value, high-sensitivity data.
- Behavior is outside normal patterns and moving fast.

03 Containment

During the Attack

Detect, Contain, Respond Faster

01 Stronger Signal

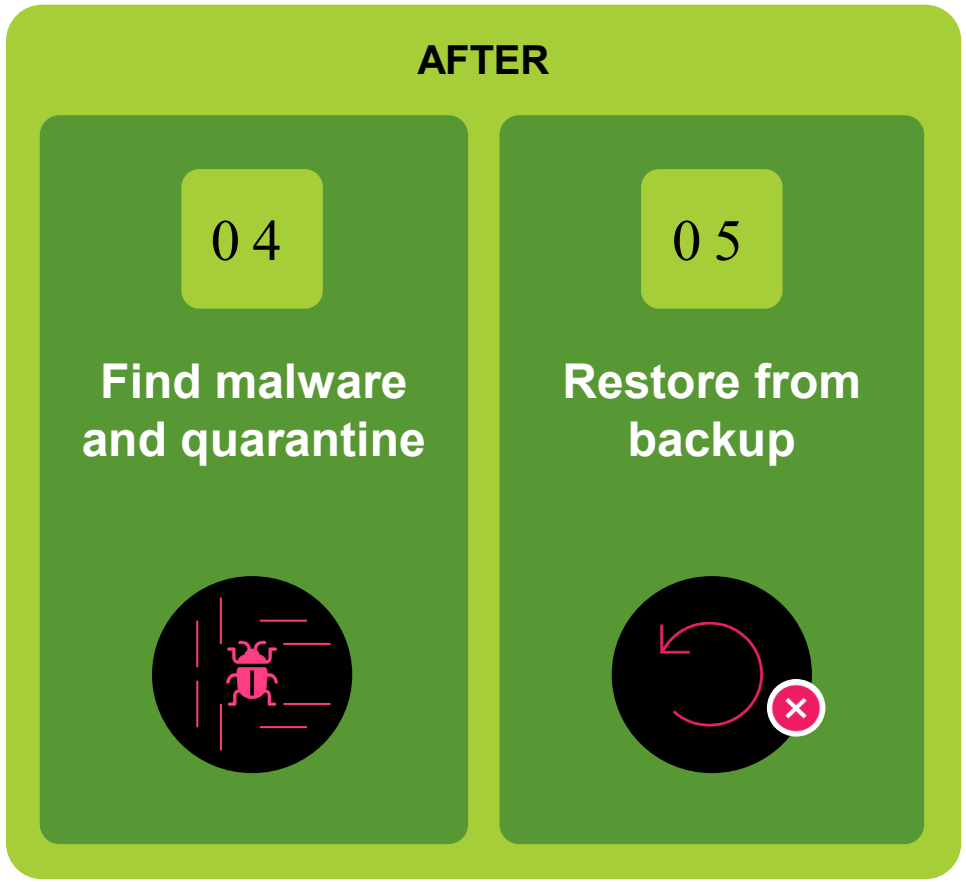
02 Prioritized Response

03 Containment

- Investigating alerts in silos.
- Correlating logs.

After the Attack

Restore Trust & Recover Faster



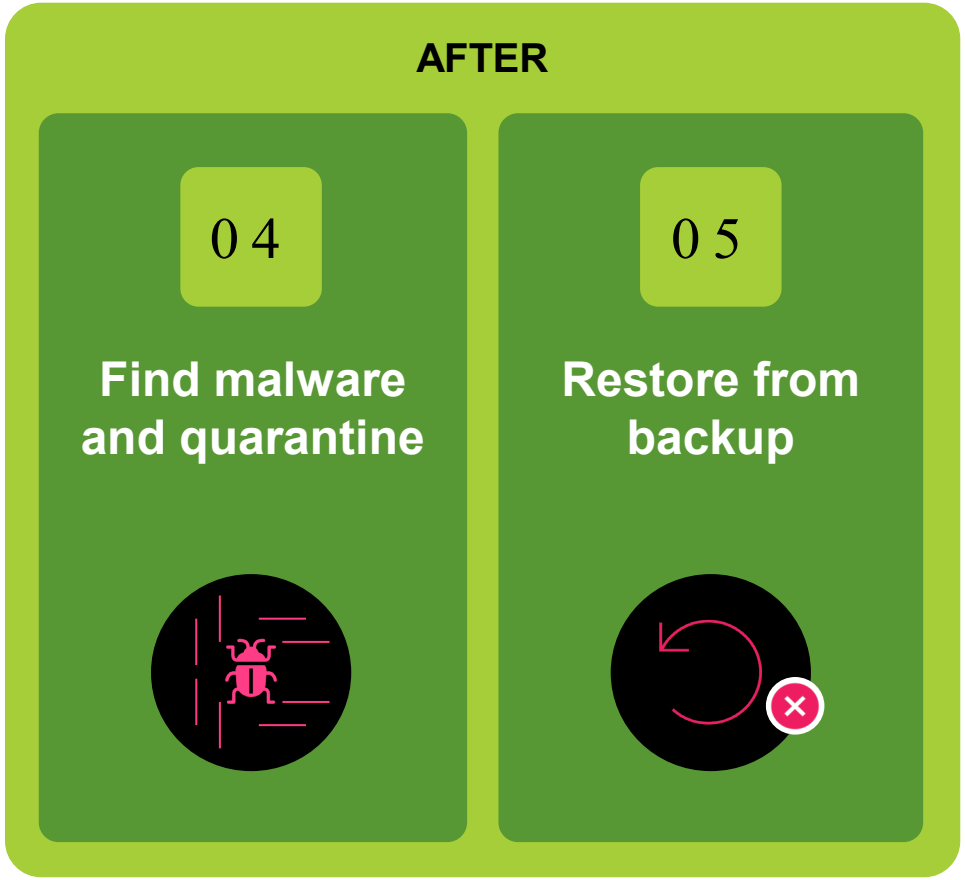
01 **Understand Blast Radius**

02 **Identify Clean Recovery Point**

03 **Eliminate Reinfection Risk**

After the Attack

Restore Trust & Recover Faster



01 Understand Blast Radius

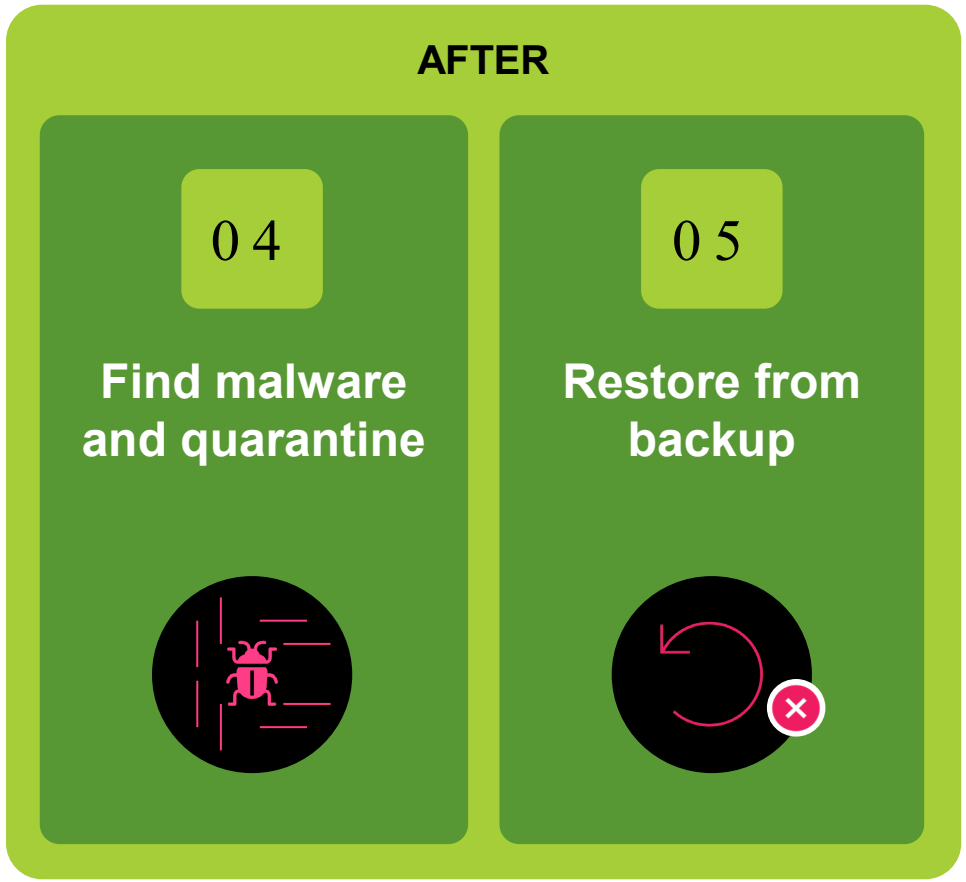
- What data was accessed or modified?
- By whom?
- How far did the attacker spread across systems and accounts?

02 Identify Clean Recovery Point

03 Eliminate Reinfection Risk

After the Attack

Restore Trust & Recover Faster



01 Understand Blast Radius

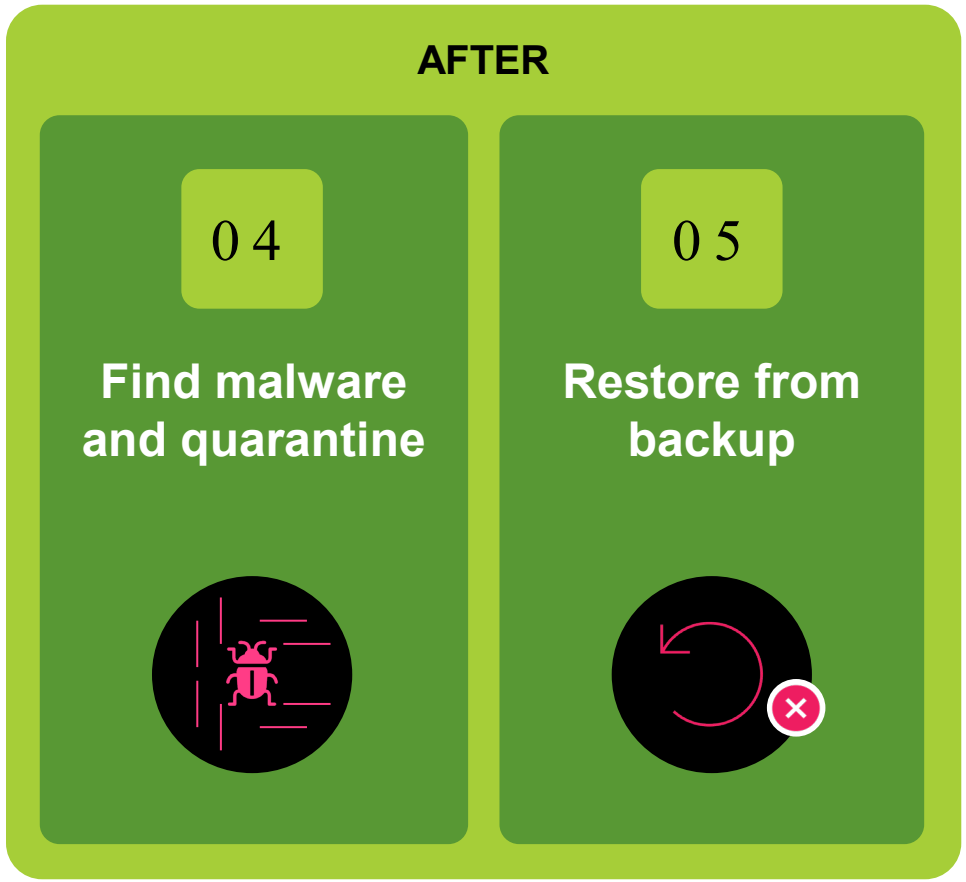
02 Identify Clean Recovery Point

- You can correlate when anomalous access began.
- You can flag data that was changed or encrypted.
- And you can restore systems to a known good state, rather than guessing.

03 Eliminate Reinfection Risk

After the Attack

Restore Trust & Recover Faster



01 Understand Blast Radius

02 Identify Clean Recovery Point

03 Eliminate Reinfection Risk

- Audit which accounts were active during the attack.
- Check for persistence mechanisms—like rogue service accounts or changes to AD.
- Validate that identities are clean before restoring access to sensitive systems.

Key Takeaways

01

Identity and data are facing the same challenges.

02

Integrated context is the foundation for resilience — before, during and after an attack

03

Resilience is critical to the strategy — not just recovery.

What's the Opportunity?

01

Map identities to sensitive data

Start by answering who can access your most critical data — and should they?

02

Right-size access before it becomes a problem

Small changes now can drastically limit attacker movement later

03

Test your resilience - not just your detection

Can we recover fast enough and cleanly enough to stop reinfection or business disruption?

Cyber Resilience means being able to successfully endure cyber attacks rather than solely trying to prevent them